IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

	)	
UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. 1:17-cr-254 (TSE)
	)	
KEVIN PATRICK MALLORY,	)	Sentencing: April 26, 2019
	)	
Defendant	)	
	)	

DEFENDANT'S SUPPLEMENTAL
MEMORANDUM IN RESPONSE TO APRIL 4, 2019
AMENDMENTS TO THE PRE-SENTENCE INVESTIGATION REPORT

Defendant Kevin Patrick Mallory, through counsel, hereby submits this Memorandum in response to this Court's Order dated April 4, 2019 (doc. 254) with respect to proposed amendments made on that date to Paragraphs 39 and 40 of the Pre-Sentence Investigation Report.

Defendant objects to the proposed revisions to paragraphs 39 and 40 of the PSR because they are unsupported by evidence adduced at the trial. Specifically, the statement in revised paragraph 39 that Mr. Mallory "intended to send . . . a document entitled FCAIS Capabilities (A) (Document 4), and . . . a document entitled FCAIS Capabilities (B) (Document 5)" to Michael Yang is not supported by the evidence. Furthermore, the statement in revised paragraph 39 that Mr. Mallory attempted "four (4) times to send Document 4" to Michael Yang is contradicted by the evidence at trial. For the send sequences recorded by the covcom device, the testimony at trial established that Mr. Mallory's username was listed as both the sender and the

recipient for send sequences associated with Document 4.   Indeed, when the government's forensic expert was asked on direct examination whether "the send steps were completed" with respect to those send sequences, he testified that "they weren't." *See* Testimony of James Hamrock, May 31, 2018 ("Hamrock Tr.") (attached as Exh. 1) at 52.

The government expert testified that these "send sequences" nonetheless evidenced an intent to send the documents to Mr. Mallory's Chinese contact based on the premise that the covcom device would crash immediately upon being placed in "secure" mode (a precursor to engaging in a send sequence) unless the device was actively connected to another device in a chat. But that premise was false: Mr. Mallory placed the covcom device in "secure mode" for an extended period during his lengthy FBI interview – while the device was entirely disconnected from any communication network – and the communication application did not crash, as evidenced by photos and testimony adduced at trial. Accordingly, the evidence regarding attempts to send Documents 4 and 5 establishes that Mr. Mallory engaged in "send sequences" with respect to those documents, but sent them to himself, and to the extent the government alleges that Mr. Mallory was nonetheless trying to send them to his Chinese contact, that claim was based on a false premise.

Moreover, the statement in revised paragraph 40 that Mr. Mallory "completed the necessary steps on the covcom device to transmit two additional documents, including the Powerpoint proposal (Document 2) and a document entitled FISA (Foreign Intelligence Surveillance Act) (Document 3)" is both contradicted by the evidence at trial and unsupported by any other evidence. This is significant because

Document 2 contained identifying information about individuals referred to at trial as "the Johnsons." The evidence at trial established that Mr. Mallory took significant steps to strip out all such identifying information from the "executive summary" document he actually sent to his Chinese contact on the same topic (Document 1), and that he never took any steps to actually send either Document 2 (which contained information that could potentially identify the Johnsons) or Document 3.

I.   Revised Paragraph 39

Revised paragraph 39 of the PSR states, in pertinent part:

At the trial, the government presented expert testimony that showed that shortly before midnight on May 1, 2017, and just after midnight on May 2, 2017 Mallory completed all of the steps necessary to transmit to Michael Yang in the PRC via the covcom device the following documents: (i) Handwritten Table of Contents describing the various documents Mallory intended to send to Michael Yang, (ii) the White Paper and handwritten notes (Document 1), (iii) a document entitled FCAIS Capabilities (A) (Document 4), and (iv) a document entitled FCAIS Capabilities (B) (Document 5). Both the Table of Contents and the White Paper contained classified information/NDI classified at the SECRET level. The two FCAIS Capabilities (Documents 4 and 5) documents contained classified information/NDI classified at the TOP SECRET level. The evidence revealed the defendant hit send four (4) times to send Document 4 and hit send one (1) time to send Document 5 to Michael Yang. . . . The evidence did not reveal whether or not Michael Yang received Documents 4 and 5.

The evidence at trial established that the document known as Document 4 was stored on an SD card as an ADOBE pdf file named, "20170425160010.pdf":

Name	Size	Type	Date Modified
.Spotlight-V100	32	Directory	4/25/2017 9:01:48 PM
.fseventsd	32	Directory	4/25/2017 9:01:48 PM
.Trashes	32	Directory	4/25/2017 9:38:24 PM
20170425155910.pdf	23	Regular File	4/25/2017 3:59:22 PM
20170425155924.pdf	312	Regular File	4/25/2017 3:59:42 PM
20170425155936.pdf	734	Regular File	4/25/2017 4:00:18 PM
20170425155955.pdf	540	Regular File	4/25/2017 4:00:34 PM
20170425160010.pdf	169	Regular File	4/25/2017 4:00:44 PM
20170425160029.pdf	326	Regular File	4/25/2017 4:00:56 PM
20170425160045.pdf	149	Regular File	4/25/2017 4:01:02 PM
20170425160103.pdf	150	Regular File	4/25/2017 4:01:20 PM
20170425160115.pdf	65	Regular File	4/25/2017 4:01:28 PM

4

FCAIS Capabilities

Gov't Ex. 9-8B (attached as Exh. 2) at 5. The numerical name of the pdf file recorded the date of creation: April 25, 2017, at 4:00:10 p.m. The same exhibit shows that Document 5 was stored as an ADOBE pdf file named "20170425160029.pdf" (suggesting that it was created 19 seconds later). *Id.*

The trial evidence also established that Mr. Mallory used the covcom device to communicate with Michael Yang by means of a common program called "WeChat," as modified by a custom application. According to the government expert's trial testimony, the "WeChat" program kept a record of transmissions in a database. *See* Hamrock Tr. (Exh. 1) at 23-24; Gov't Ex. 8-18 (attached as Exh. 3). Government Exhibit 8-18 is copy of a table from this database showing transmissions on May 1, 2017:

Date	id	uploadsrc	from	to	ori	cmdtype	prog	Source File
2017-05-01 -4.0 22:54:16.802	16	0	wxid_co76ckxd7nie22	wxid_p7df2fo4b5lw22	/storage/emulated/0/sdir/20170425155910.jpg	1	com.tencent.mm.y.o@3599eb49	MM_20170501.xlog_conv
2017-05-01 -4.0 23:08:15.208	17	0	wxid_co76ckxd7nie22	wxid_p7df2fo4b5lw22	/storage/emulated/0/sdir/20170425155924.jpg	1	com.tencent.mm.y.o@10a683b3	MM_20170501.xlog_conv
2017-05-01 -4.0 23:15:24.740	18	0	wxid_co76ckxd7nie22	wxid_co76ckxd7nie22	/storage/emulated/0/sdir/20170425160010.jpg	1	com.tencent.mm.y.o@10615a1e	MM_20170501.xlog_conv
2017-05-01 -4.0 23:30:45.959	23	0	wxid_co76ckxd7nie22	wxid_co76ckxd7nie22	/storage/emulated/0/sdir/20170425160010.jpg	1	com.tencent.mm.y.o@1a5e45ad	MM_20170501.xlog_conv
2017-05-01 -4.0 23:39:25.445	24	0	wxid_co76ckxd7nie22	wxid_co76ckxd7nie22	/storage/emulated/0/sdir/20170425160010.jpg	1	com.tencent.mm.y.o@1a5ef692	MM_20170501.xlog_conv
2017-05-01 -4.0 22:52:01.083					/storage/emulated/0/sdir/20170425155910.jpg			TOOL_20170501.xlog_conv
2017-05-02 -4.0 00:03:04.614					/storage/emulated/0/sdir/20170425155924.jpg			TOOL_20170502.xlog_conv

Gov't Ex. 8-18 (Exh. 3).

This table shows, for example, that on "May 1st 22:54:16 that a JPEG image was sent from user ending in the E22 to User W22." Hamrock Tr. (Exh. 1) at 24. At trial, the government introduced Exhibit 8-23 showing that Mr. Mallory's username in the database was "wxid_co76ckxd7ni**e22**," while Mr. Yang's was "wxid_p7df2fo4b5l**w22**":

Gov't Ex. 8-23 (attached as Exh. 4). Accordingly, with respect to the transmission at that time (the first entry in the chart above), the evidence established: i) that it was from Mr. Mallory's user ID to Mr. Yang's; and ii) that the filename of the document sent ("20170425155910.jpg") corresponds to the document known as the Table of Contents. *See* Gov't Ex. 9-8B (Exh. 2) at 1.

All of the logs kept by the WeChat application, however, with respect to transmissions associated with Document 4 show that it was sent *from* user ending in E22 (Mr. Mallory) *to* the user ending in E22 (Mr. Mallory):

2017-05-01 -4.0 23:15:24.740	18	0	wxid_co76ckxd7nie22	wxid_co76ckxd7nie22	/storage/emulated/0/sdir/20170425160010.jpg
2017-05-01 -4.0 23:30:45.959]	23	0	wxid_co76ckxd7nie22	wxid_co76ckxd7nie22	/storage/emulated/0/sdir/20170425160010.jpg
2017-05-01 -4.0 23:39:25.445	24	0	wxid_co76ckxd7nie22	wxid_co76ckxd7nie22	/storage/emulated/0/sdir/20170425160010.jpg

Gov't Ex. 8-23 (Exh. 4).   In other words, unlike the first two documents that the

WeChat database recorded as transmitted from Mr. Mallory to Michael Yang – which

correspond to the Table of Contents and Document 1 – the WeChat log entries

associated with the transmissions of Document 4 show that they were sent to and

from the same username ending in "nie22" – Mr. Mallory's.   *Id.*

At trial, government counsel asked Mr. Hamrock during his direct examination

about the fact that these logs showed the same username in the "to" and "from"

columns, and he testified that it meant that the send sequences were not completed:

> Q.   What does the fact that the next three have the same
> to and from suggest to you about whether the send steps
> were completed?
>
> A.   *They weren't.* They could have been completed, but
> it could have timed out.

Hamrock Tr. (Exh. 1) at 52 (emphasis added).   Nonetheless, the government

contended that these sequences must have been attempted transmissions to Mr. Yang

because, according to Mr. Hamrock, the system would crash if one entered the "secure

mode" without being in active contact with another device on the WeChat network.

See Hamrock Tr. (Exh. 1) at 36 ("as soon as you hit the password and it comes up with

the exclamation point, it's been hooked, but it realizes it's not communicating out on

WeChat to the other individual so it crashes.").   For this reason, he testified that

"send sequences" could have been executed only when in a "chat session

communicating with somebody else." *Id.* at 37.

That conclusion was incorrect. During Mr. Mallory's FBI interview, the covcom phone was placed in "airplane" mode – so that it was not communicating with any other user – and then Mr. Mallory showed the FBI agents how to enter the "secure mode" by entering the password and revealing texts beginning with an exclamation point:

GX 8-5 (attached as Exh. 5).

Accordingly, the evidence at trial with respect to Documents 4 and 5 did *not* establish that Mr. Mallory "completed all the steps necessary to transmit [those documents] to Michael Yang," as asserted in revised paragraph 39. Indeed, the government's expert testified that those steps were *not* completed, and that conclusion is supported by the content of the text message communications between Mr. Mallory and Mr. Yang, which contain no mention of either Document 4 or 5 being sent, received, or attempted to be sent.

II.   Revised Paragraph 40

Revised paragraph 40 states, in pertinent part:

The government also presented expert testimony that revealed that several days later, on May 5, 2017, Mallory completed the necessary steps on the covcom device to transmit two additional documents,

including the PowerPoint proposal (Document 2) and a document entitled FISA (Foreign Intelligence Surveillance Act) (Document 3).

There is, however, no indication that Document 2 or 3 were ever sent. There are no "send sequences" relating to those documents, and the content of the chat transcript makes clear that Mr. Yang never received them. By way of background, the parties agree that Mr. Mallory, on May 1, 2017, sent Mr. Yang a "white paper" known as Document 1, which is a short summary of the operation described in the PowerPoint presentation known as Document 2. But while Document 2 contained information that could have led to the identification of the "Johnsons," the trial evidence established that the author of the "white paper" (Document 1) excluded from it all of the information in Document 2 that might have led to the identification of the "Johnsons" or to any other intelligence asset. *See* Testimony of Hugh Higgins, June 5, 2018 ("Higgins Tr.") (attached as Exh. 6), at 76-78.

Indeed, after reviewing the short "white paper" known as Document 1, Mr. Yang sent Mr. Mallory a message on May 3, 2017, at 11:27:40 p.m., requesting that he send Document 2 and Document 3:

related and it's too simple, pls at least
send the no2 ███████████████
and the FISN...otherwise I will be in a
extremely awkward situation

!:Ok. Have a good weekend

Gov't Ex. 8-6 (attached as Exh. 7), lines 84 & 85. On May 5, at 6:06:51 and 6:08:09 p.m., Mr. Mallory typed the following texts, suggesting that he was sending Documents 2 and 3:
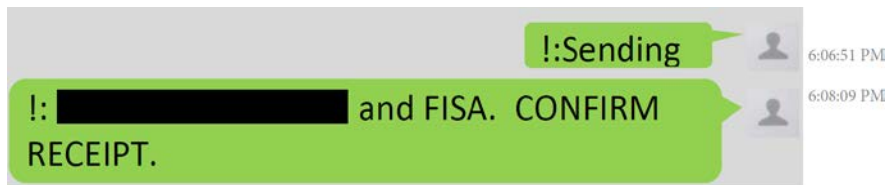
Id. at lines 87-88. Importantly, however, Mr. Hamrock's analysis of the covcom device shows no send sequences associated with those times. Moreover, there are no send sequences at any time associated with the files known as Document 2 and Document 3. *See* Gov't Ex. 8-21(attached as Exh. 8) at 8 (detailing "send sequences" on May 5, 2017, but none at or near 6:08 p.m., and none associated with Documents 2 or 3).

Later that evening, Mr. Yang indicated that he had not received Documents 2 and 3, and asked that they be resent:

Gov't Ex. 8-6 (Exh. 7), line 100.

Mr. Mallory declined, stating:
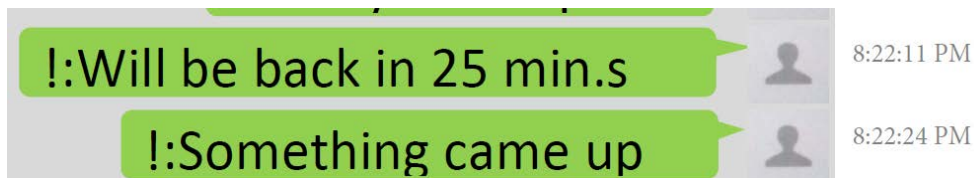
Id. at lines 104-05. But even thereafter, Mr. Mallory never executed any send sequence associated with Documents 2 or 3.

Later that evening, Mr. Mallory did execute send sequences, but the trial evidence was clear in multiple ways that they were not associated with Documents 2 or 3. The context for these transmissions starts on May 3, at 10:43:34, when Mr. Yang wrote the following text:

> !:He's interested in the products. But no1 is
> incomplete on the the first page and the
> handwriting cannot be read properly

Gov't Ex. 8-6 (Exh. 7), line 17. Later in the same conversation, Yang wrote:

> !:Anyway, I suggest you send all and retype
> the handwriting. And NO1 is obvious the
> first page of an complete article, where's
> the else and why it is black on top.and
> bottom

Id. at line 34. In these text messages, Mr. Yang noted that handwritten notes (determined to be unclassified) previously sent by Mr. Mallory were illegible, and asked him to "retype the handwriting." Mr. Mallory responded at 11:27:29 in the same conversation:

> !:I will typa notes and resend by Sat. I am travelling for next few days on DOD project.

Id. at line 83.

On May 5, 2017 at 6:09 p.m. (about 90 seconds after Mr. Mallory typed a message claiming to send Documents 2 and 3, but without any corresponding send sequences), Mr. Mallory stated as follows:

> !:I will type two pages of notes (no. 1) and send later today or tomorrow.   6:09:47 PM

Gov't Ex. 8-6 (Exh. 7) at line 89. Approximately forty-five minutes later, Mr. Mallory sent the following text messages:
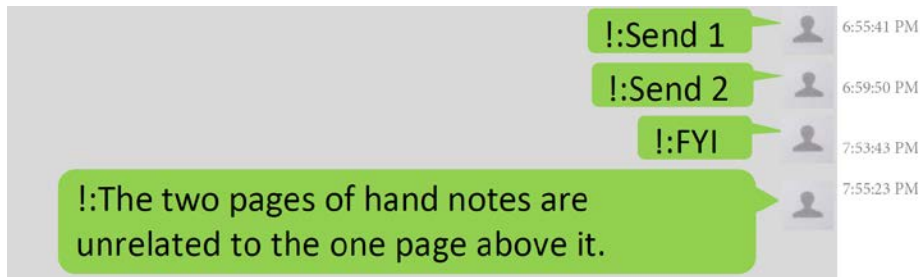
Id. at line 92-95. Moreover, the covcom device logged send sequences that correspond

with the exact times of those text messages:

shows image sent at times just after the user types Send1:

| 92 | 2017-05-05 **18:55:41** | wxid_p7df2fo4b5lw22 | Outgoing | Send 1 |

shows image sent at times just after the user types Send2:

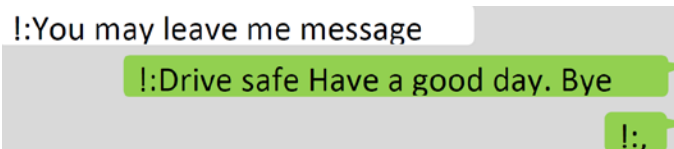| 93 | 2017-05-05 **18:59:50** | wxid_p7df2fo4b5lw22 | Outgoing | Send 2 |

Gov't Ex. 8-21 (Exh. 8) at 8 (detailing May 5 send sequences). But the filenames

associated with the "image(s) sent" in connection with those messages do not

correspond with Documents 2 or 3, or any other classified document. *See* Hamrock

Tr. (Exh. 1) at 78.

Given the context of the text messages in which Mr. Mallory stated that he

would send typed versions of the handwritten notes previously sent, the government's

forensic expert testified at trial that, based on his forensic analysis, these two

transmissions appeared to relate to "the two pages of hand notes that it correlates to

probably one of those two." *See* Hamrock Tr. (Exh. 1), at 75 line 22 through 78 line

12.

Later that evening, at 9:03:06, Mr. Yang wrote:

Mr. Mallory responded, "Ok." Gov't Ex. 8-6 (Exh. 7) at lines 127-28. Mr. Yang and

Mr. Mallory then discuss engaging in more limited contacts, reimbursement for Mr.

Mallory, and the possibility of a visit by Mr. Mallory in June. Shortly thereafter, on

May 5, 2017 at 9:34 p.m., Mr. Mallory and his Chinese contact terminated their

discussion without Mr. Mallory having taken any further steps to send documents,

and they never again communicated using the covcom device:

See GX 8-6 (Exh. 7) at lines 161-63; Hamrock Tr. (Exh. 1) at 81 (covcom device last

used on evening of May 5-6, 2017). By that time, of course, Mr. Mallory had

communicated with a contact at the CIA to set up a meeting.

The trial evidence, therefore, shows that Mr. Mallory never sent or attempted

to send Document 2 (the PowerPoint with information about the Johnsons) or

Document 3. Rather, Mr. Mallory sent only the Table of Contents and Document 1,

which was a short summary of Document 2 that excluded all potentially identifying

information associated with the Johnsons. Then, when Mr. Yang specifically

requested that he send Documents 2 and 3, Mr. Mallory sent texts messages

purporting to send Documents 2 and 3, but no corresponding send sequences

occurred, and none *ever* occurred corresponding with the filenames associated with

Documents 2 or 3. And when Mr. Yang later asked that Documents 2 and 3 be re-

sent because he had not received them, Mr. Mallory said he could not send them

because "something came up." Finally, the send sequences associated with the text

messages in which Mr. Mallory wrote "Send 1" and "Send 2" do not reflect any connection with Documents 2 or 3, and the context and trial testimony establish that those texts, and corresponding send sequences, relate instead to typed versions of unclassified handwritten notes.

Dated: April 11, 2019   Respectfully submitted,

                                                KEVIN PATRICK MALLORY

                                                By Counsel,

                                                By: _____/s/_____
                                                Geremy C. Kamens
                                                Va. Bar. No. 41596
                                                Todd Richman
                                                Va. Bar No. 41834
                                                Office of the Federal Public Defender
                                                Attorneys for Mr. Mallory
                                                1650 King Street, Suite 500
                                                Alexandria, VA 22314
                                                (703) 600-0848 (T)
                                                (703) 600-0880 (F)
                                                Geremy_Kamens@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on April 11, 2019, I will electronically file the foregoing pleading with the Clerk of the Court using the CM/ECF system, which will then send a notification of such filing (NEF) to:

John T. Gibbs, Esq.
Colleen E. Garcia, Esq.
Assistant United States Attorneys
2100 Jamieson Avenue
Alexandria, VA 22314

Jennifer K. Gellie, Esq.
Trial Attorney
United States Department of Justice
600 E. St., NW
Washington, DC 20004

<div style="text-align: right;">

/s/
Geremy C. Kamens
Va. Bar No. 41596
Federal Public Defender
Attorney for Mr. Mallory
Office of the Federal Public Defender
1650 King Street, Suite 500
Alexandria, VA 22314
(703) 600-0848 (T)
(703) 600-0880 (F)
Geremy_Kamens@fd.org

</div>